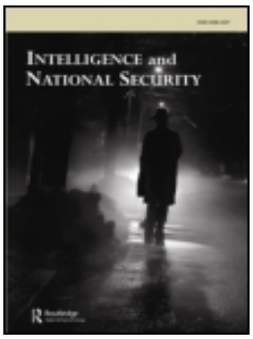

Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: www.tandfonline.com/journals/fint20

TICOM: The Last Great Secret of World War II

Randy Rezabek

To cite this article: Randy Rezabek (2012) TICOM: The Last Great Secret of World War II, Intelligence and National Security, 27:4, 513-530, DOI: 10.1080/02684527.2012.688305

To link to this article: https://doi.org/10.1080/02684527.2012.688305

Published online: 27 Jul 2012.

Submit your article to this journal

Article views: 928

View related articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=fint20

Intelligence and National Security
Vol. 27, No. 4, 513–530, August 2012

Routledge
Taylor & Francis Group

TICOM: The Last Great Secret of World War II

RANDY REZABEK*

ABSTRACT Recent releases from the National Security Agency reveal details of TICOM, the mysterious 1945 operation targeting Germany's cryptologic secrets. Often mentioned by such authors as Kahn, Bamford, Parrish and Aldrich, for the first time the public has access to this information. This article provides a review in greater depth than has been previously covered in the open literature of the history of the TICOM operation, and its resulting intelligence, including the Germans' efforts against Soviet communications. In addition, some comments are provided on why TICOM has remained classified long after other similar information from World War II was declassified, and why locating TICOM documents is still difficult.

For decades, allusions to the mysterious TICOM (Target Intelligence Committee) operation of 1945 appeared in the literature of signals intelligence, but few details beyond anecdotes from participants or glimpses into classified documents were published. Finally, the secrets are beginning to leak. Quietly, a few years ago, the National Security Agency (NSA) began declassifying information concerning TICOM. Conducted in the wake of the European victory, this intelligence operation documented the signals intelligence effort of the German state, and resulted in an archive of information considered so sensitive that it remained Top Secret for the next 65 years.

The historiography of TICOM is brief and recent. The whole subject of cryptology was largely unknown to the public until the 1974 publication of *The Ultra Secret* by F.W. Winterbotham, which in the next decade encouraged a flood of memoirs and histories on the Ultra program.[1] Despite this torrent of information, there was no mention of TICOM until Thomas Parrish's 1986 account in *The Ultra Americans*.[2] His history of the American role in Bletchley Park's Ultra program is the earliest published account of TICOM that has been available in the open literature. James

*Email: rrezabek@rochester.rr.com
[1]F.W. Winterbotham, *The Ultra Secret* (London: Weidenfeld and Nicolson 1974).
[2]Thomas Parrish, *The Ultra Americans* (New York: Stein and Day 1986).

ISSN 0268-4527 Print/ISSN 1743-9019 Online/12/040513-18 © 2012 Taylor & Francis
http://dx.doi.org/10.1080/02684527.2012.688305

Bamford's 2001 book, *Body of Secrets: Anatomy of the Ultra-secret National Security Agency*, the second in his widely read series of books on signals intelligence, has a chapter containing one of the most complete accounts of the TICOM mission available. Bamford declared that: 'The organization was so secret that even today, more than half a century later, all details concerning its operations and activities remain classified higher than Top Secret … making TICOM probably the last great secret of the Second World War'.[3] Richard J. Aldrich's *The Hidden Hand: Britain, America, and Cold War Secret Intelligence* adds additional details about the TICOM mission with additional information on German sigint (signals intelligence) officers captured and held for debriefing.[4] And Paul Whitaker, one of the TICOM officers, and Louis Kruh, teamed up to write a 1987 article that is unique in that it presents a series of unofficial photographs taken by Whitaker on the mission, including scenes of the discovery of the 'Russian Fish'.[5]

Of these sources, only Bamford cites the official Army 1946 study of TICOM, still classified at the time of his writing. In the summer of 2010, it was finally released to the public when it was posted on the NSA's website, finally opening up details of this secretive intelligence operation conducted in the closing days of World War II.[6]

The main purpose of this article is to provide a review of the history of the TICOM operation in greater depth than has been previously covered in the open literature, and it will provide an in-depth description of the intelligence collected by the operation. In addition, the article will review some issues relating to why TICOM had remained classified long after other similar information from World War II was declassified, and why locating its documents is still difficult.

Allied planning for the occupation of Europe in the event of a sudden German collapse began as early as August 1943. As part of this effort, a number of intelligence operations were planned to seize the intellectual property of the Third Reich. Loosely coordinated by the Combined Intelligence Objectives Subcommittee a number of missions under various codenames and with different targets were planned, such as Alsos, which searched for nuclear information and research, Overcast, dedicated to the capture of rockets, and Surgeon, looking for avionics and jet technology.

---

[3]James Bamford, *Body of Secrets*: *Anatomy of the Ultra-Secret National Security Agency* (New York: Anchor Books 2001) pp.7–21.

[4]Richard J. Aldrich, *The Hidden Hand: Britain, America, and Cold War Secret Intelligence* (Woodstock; New York: The Overland Press 2001).

[5]Paul Whitaker and Louis Kruh, 'From Bletchley Park to Berchtesgaden', *Cryptologia* 11 (1987), pp.129–41.

[6]National Security Agency, *European Axis Signal Intelligence in World War II as Revealed by 'TICOM' Investigations and by Other Prisoner of War Interrogations and Captured Material, Principally German*, WDGAS-14, Chief Army Security Agency, Top Secret/Cream report, 1 May 1946, nine volumes (hereafter referred to as TICOM), <http://www.nsa.gov/public_info/declass/european_axis_sigint.shtml> (accessed 15 June 2010).

These operations became well known in both popular and academic literature.[7] However, a lesser known operation, TICOM, targeted the capture of German signals intelligence and to this day remains shrouded in mystery.

Colonel George A. Bitcher, the senior US signals intelligence officer in the European Theatre of Operations, initiated American participation in TICOM. Upon learning of the British planning, Bitcher determined that Americans needed to be included in the operation and he began working the chain of command. This resulted in a memo from Army Chief of Staff George Marshall directing General Dwight Eisenhower to form a team to participate with the British. Marshall's memo defined four objectives for the TICOM mission: to learn the extent of the German cryptanalytic effort against England and America; to prevent the results of such German effort from falling into unauthorized hands as the German Armies retreated; to exploit German cryptologic techniques and inventions before they could be destroyed by the Germans. Finally, to uncover items of signal intelligence value in the war against Japan was a major concern[8]. It was in effect, a shopping list from Marshall for any and all information pertaining to German secret communications.

The collection effort began in April 1945, when six teams, with representatives from the British GC&CS (Government Code and Cipher School), the US Army's ASA (Army Security Agency), and the US Navy's OP-20G, drawn largely from the personnel at Bletchley Park, deployed to the continent. The original operation, planned earlier that spring, called for these TICOM teams to jump into Berlin with the 101st Airborne division, seize the headquarters of German signals intelligence agencies, and then hope the paratroopers could defend them until relieved by an American armored column from the west. Changing circumstances on the ground by March canceled this operation.[9] For these desk-bound and largely scholarly professorial types in the cryptologic service, this change of plan must have been a relief.

Traveling across war-torn Germany these teams scored a number of successes. TICOM Team 6 was the first sent out, to north Germany in the Heumenster–Ploen–Flensburg area that was overrun by the British. The team managed to capture and exploit the German Naval Signals Intelligence Agency (OKM/4 SKL/III, the B-Dienst) headquarters.

Then in March 1945 a US Army unit advancing into Saxony captured a castle at Burgscheidungen that contained the German Foreign Service Sigint archive, including a number of broken Russian codes and ciphers. Since this castle was in the proposed Soviet zone, TICOM quickly dispatched Team

[7]Tom Bower, *The Paperclip Conspiracy* (Boston, MA: Little, Brown and Company 1987); Matthew Uttley, 'Operation "Surgeon" and Britain's Post-War Exploitation of Nazi German Aeronautics', *Intelligence and National Security* 17/2 (2002) pp.1–26.
[8]TICOM, *Volume 1 – Synopsis*, 3.
[9]Parrish, *The Ultra Americans*, pp.272, 275–6.

3.[10] According to team member Major Paul E. Neff, one of the American cryptologists from Bletchley Park, the most difficult part of the mission was getting diplomatic permission from the British to evacuate the German personnel to England for interrogation.[11]

However, the greatest success was found in Bavaria. Just a few days before the German surrender, TICOM team 1 consisting of American officers Paul Whitaker, Selmer Norland, Arthur Levenson and Howard Compaigne, five British intelligence officers, two radio operators and two drivers were dispatched.[12] One of the goals of this team was to capture intact a T-52 *Geheimschreiber* (secret writer), a sophisticated, on-line encrypted teletype device that was used to generate the German high command cipher codenamed 'Fish' by the British.[13] At a Luftwaffe communications center in Kaufbeauren, the team found a number of T-52s, but to their disappointment the machines were smashed and their rotors missing. This site also turned out to be the evacuated headquarters of the FA (Forschungsamt), better known as Herman Goering's Research Bureau, the Nazi Party's in-house cryptologic service. Later a side group of the team under the famous British cryptologist Major Ralph Tester found an intact T-52 machine in the town of Pfunds, 40 miles southwest of Innsbruck. A few days later near Berchtesgaden, an Army task force captured Field Marshal Kesselring's communications train, a convoy of four German signal trucks complete with Fish machines and their operating personnel. Turned over to TICOM, Tester and Levenson decided to accompany this convoy on the long drive back to the channel ports, guarded by their own prisoners.[14]

While Tester and Levenson went on their adventure across war-torn Europe, the rest of the TICOM team moved further east to Rosenheim to interview some prisoners who had served at OKH/GdNA, the sigint agency of the German Army. Anxious to avoid being turned over to the Russians, they revealed the existence of a new device designed to intercept a new Soviet high-level communications that split the message onto nine different channels that were transmitted on a broader spectrum of frequencies, which made interception difficult. This device, buried nearby, was nicknamed 'the Russian Fish', by TICOM. The next day the German prisoners dug up seven-and-a-half tons of equipment and materials and set it up to demonstrate to the TICOM team. This device and its accompanying German technicians were sent back to England.[15]

---

[10]NARA, *Final Report of TICOM Team 3 on Exploitation of Burgscheidungen*, RG 457, 570, A, 67, 2, Box 44.

[11]Bamford, *Body of Secrets*, p.11.

[12]Parrish, *The Ultra Americans*, p.278; Whitaker and Kruh, 'From Bletchley Park to Berchtesgaden', pp.129–41.

[13]Bamford, *Body of Secrets*, p.14.

[14]Parrish, *The Ultra Americans*, pp.280–2; R.D. Farley, 'Oral History Interview with ARTHUR J. LEVENSON', NSA-OH-40-80, 25 November 1980, Ft. Meade Maryland, National Security Agency, Center for Cryptologic History, <http://www.nsa.gov/public_info/_files/oral_history_interviews/nsa_oh_40_08_levenson.pdf> (accessed 15 May 2010).

[15]Parrish, *The Ultra Americans*, pp.282–6; Bamford, *Body of Secrets*, pp.15–17; Whitaker and Kruh, 'From Bletchley Park to Berchtesgaden', pp.129–41.

The other teams also scored success that was perhaps less spectacular, but still useful. Team 2, dispatched to the Innsbruck and Pilsen areas, exploited the captured German Army sigint regiment KONA 1. Team 4 searched the Ebermannstadt area of south central Germany in an unsuccessful effort to discover the archive of OKW/*Chi*. However, they did capture the Laboratory Feuerstein, an important signals research and development site. Team 5 was a small two-man detachment dispatched to supervise diving teams at Lake Schliersee, where the archives of OKW/*Chi* were finally recovered.

We can only speculate about the impact of the TICOM teams on the early Cold War. However, to have the Russian Fish machine intercepting traffic as early as June 1945, along with all the other German research and decrypts must have been instrumental in the immediate post-war Anglo-American intelligence effort against the Soviet Union. In addition to the Russian codes, the TICOM materials assisted the United States in its ability to read the secure communications of dozens of other countries, including Argentina, France, Czechoslovakia, Romania, Spain and Yugoslavia.[16] In addition, a number of high-level German sigint personnel identified and interrogated by the Allies, including Dr. Erich Huettenhain, who later became the top code-breaker for the West German post-war Gelhan organization, Generalmajor Klemme, commander of Luftwaffe radio intelligence, and fellow Luftwaffe officers Lieutenant Colonel Friedrich, and Majors Oeljeschaeger and Beulmann of the Crypto planning branch.[17] Hundreds of these Nazi code-breakers processed through a secret interrogation center codenamed 'Dustbin'.[18]

Because of the teams' efforts, by May 1946 the Army Security Agency produced the nine-volume study containing the intelligence summary of the TICOM operation. Among the volumes are descriptions of the organization and operation of five German signal intelligence agencies, analysis of German high-level cryptology and cryptanalysts efforts, and a volume discussing the German traffic analysis of Russian communication systems.[19] Of great value to historians, is a glossary in each volume listing a total of over 200 other intelligence reports, most produced by TICOM, that were the sources of information for this study.[20]

TICOM studied the history, organization, field operations, and liaison relationships of five of the German's signal intelligence agencies: the

[16]Bamford, *Body of Secrets*, p.19.
[17]Aldrich, *The Hidden Hand*, p.238.
[18]Bamford, *Body of Secrets*, p.17.
[19]TICOM, *Volume 2 – Notes on German High Level Cryptography and Cryptanalysts*; TICOM, *Volume 3 – Signal Intelligence Agency of the Supreme Command, Armed Forces*; TICOM, *Volume 4 – Signal Intelligence Service of the Army High Command*; TICOM, *Volume 5 – The German Air Force Signal Intelligence Service*; TICOM, *Volume 6 – Foreign Office Cryptanalytic Section*; TICOM, *Volume 7 – Goering's Research Bureau*; *TICOM, Volume 9 – German Traffic Analysis of Russian Communications.*
[20]TICOM, *Volume 1 – Synopsis*, p.4.

Supreme Command of the Armed Forces (abbreviated OKW/*Chi*[21]); the Army (after a series of name changes, ultimately known as the OKH/GdNA[22]); the Air Force (abbreviated OB d L, but commonly known as *Chi* Stelle[23]); the Foreign Office Cryptanalytic Section (Personal Z Sonderdienst, or Pers ZS); and the Nazi Party's sigint agency, the Research Bureau (Forschungsamt, the FA).

Among the military, the OKW/*Chi* was the highest agency in the hierarchy. However, its power to coordinate and set policy for the rest of the military signal intelligence organizations was limited, and mainly concentrated on cryptology, that is the creation of the German's own secure communications systems. As far as cryptanalysts were concerned, OKW/*Chi* acted as a troubleshooter, providing high-level assistance for those systems that were unsolvable by the individual services themselves.

The roots of the OKW/*Chi* lie in the post-World War I cipher section of the Defense Ministry created in 1920 and staffed by cryptologic veterans of the war. With the rise of the Nazis and the formation of the Wehrmacht as the Armed Forces Supreme Command, this unit grew. By 1937 the OKW/*Chi* had 40 employees, grew to almost 200 by the outbreak of the war, and by 1944 its central organization had an establishment of 800 personnel.[24] By this time, its emphasis had shifted to the strategic with an emphasis on diplomatic and broadcasting traffic.[25]

OKW/*Chi*, organized into four principal groups, was concerned with liaison, cryptanalysts and translation, interception, and intelligence. The cryptanalytic section was composed mainly of linguists, but also had a dedicated mathematical section and concentrated on the more challenging ciphers. The interception group, with stations at Ludwigsfelds, Treuenbrietzen and Lauf, was primarily concerned with monitoring foreign news broadcast and news services prepared a daily foreign news summary and intercepted encrypted diplomatic Morse networks. The intelligence section was responsible for evaluating and distributing broken and translated messages, and controlled the agency's archives. Development and control of secure cryptologic systems, the responsibility of its Cryptologic section, was limited to the military and a few minor government agencies.[26] This lack of a centralized authority over cipher security must have been a contributing factor to the insecurity of many German systems, including the Enigma.

In terms of cryptanalysts, the agency did achieve a series of minor success and was able to keep a steady flow of intelligence to the high command.[27] They maintained a large section, up to 40 to 50 persons, dedicated to

[21]In German, Oberkommando der Wehrmacht Chiffrierabteilung.
[22]Oberkommando des Heeres/ General der Nachrichten Aufklaerung.
[23]Chiffrier Stelle, Oberbefehlshaber der Luftwaffe.
[24]David Alvarez, 'Wilhelm Fenner and the Development of the German Cipher Bureau, 1922–1939', *Cryptologia* 31/2 (2007) pp.152–63; TICOM, *Volume 1 – Synopsis*, p.18.
[25]TICOM, *Volume 3*, pp.13–14.
[26]Ibid., p.19.
[27]TICOM, *Volume 3*, p.55.

attacking Anglo-American communications. OKW/*Chi* made breaks into the diplomatic American strip system and possibly some military attaché M-209 traffic. They had a role in the effort to read the American military attaché in Cairo's system that was vital to Rommel's campaign. Other US diplomatic systems were attacked, including a five-letter system, and an unenciphered codebook of about 100,000 groups was read. There was successful work done against the British Interdepartmental Cipher; however, no high-level American or British machine ciphers were attacked successfully and OKW/*Chi* soon gave up its attempts. The Russian section of OKW/*Chi* was small and seems to have accomplished little.

OKW/*Chi* began to disintegrate at the end of the war. Sections were moved out of Berlin and by April most of the agency's personnel began to move toward south Germany, breaking up into different transport trains, with most of them ultimately ending up at Werfen, near Salzburg, where they were captured by American troops. Some of the leadership of the agency went north to join the remnants of the German government near Flensburg, where the British arrested them.

In common with OKW/*Chi*, the Army Signal Intelligence Service (known as Inspectorate 7/VI until the reorganization of 1944, thereafter known as OKH/GdNA) had its common roots in the pre-Hitler era Code and Cipher section of the Defense Ministry. OKH/GdNA's mission was the interception and analysis of foreign military communications. This was a large organization, numbering over 12,000 personnel by the height of the war, many of them assigned to GdNA's extensive tactical field based interception and analysis units.

By the mid point in the war, GdNA's central organization was composed of three branches. IN 7/VI itself in Berlin; a central evaluation agency, the LNA, which was dedicated to analysis of traffic from numerous nations including the United States, Britain, Italy, and the Balkans, located at Zossen; and additionally, from 1941, a center dedicated to the analysis of Russian traffic in East Prussia, the Intercept Control Station East (HLS Ost). Due to bombings and retreats, the three centers reorganized and centralized into one agency for cryptanalysts and evaluation in October 1944 with the formation of the GdNA.

The German Army's field signal intelligence effort was organized into nine sigint regiments (known as KONAs) stationed on every front. They provided a full set of services including interception, traffic analysis, direction finding and evaluation and translation services to provide tactical intelligence to their assigned Army groups. New KONAs were formed during the war as the strategic situation changed when new fronts were created by Allied invasions and the Germans were put on the defense.[28]

The Army put much effort into the interception of Russian traffic with three KONAs assigned to cover the Eastern Front, including a special detachment in Finland. Following their traditional offensive philosophy, these units operated as far forward as was practicable, with one regiment,

[28]TICOM, *Volume 4*, p.42.

KONA 2 caught in a pocket and captured intact by the Russians in 1945.[29] Although many low-grade Soviet systems were read, TICOM concluded that the majority of the German sigint success on the Eastern Front was a result of skillful use of traffic analysis.

On the Western Front, coverage was concentrated initially on Allied traffic originating from the British Isles, Iceland and the continental United States. During the Norway campaign Army cryptanalysts captured a copy of the British War Office code and successfully read this code from 1941 until 1943. IN 7/VI also expended a great deal of effort to solve the British high-level system TYPEX, but made little progress, finally abandoning the effort sometime in 1943. In North Africa, a Long Range Sigint company, FAK 621, provided tactical and strategic intelligence to General Rommel and was a key factor in his early victories in the campaign. The company was captured in part by the British in July 1942, after which Rommel's success steadily declined.[30]After D-Day, the emphasis naturally shifted to coverage of British, American and French traffic emanating from the front.

As for their efforts against the Americans, a number of four-figure administrative codes used primarily in traffic from Iceland or the Mediterranean were solved. Early in the war, they broke an old US Army cipher named M-94, purely through mathematical analysis. However TICOM reports that 'after the solution had been achieved cryptanalytically, a USA manual (FM 11-5) with a complete description of the M-94 was found in a Berlin library'. The successor to the M-94 was a Hagelin type machine called the M-209, solved by the Germans in the autumn of 1943. This medium-level cipher represented the outstanding success of IN 7/VI against the Americans. Captured codebooks containing M-209 settings proved to be of great tactical value, and the M-209 keys of the 82nd and 101st Airborne divisions were captured during the D-Day invasion, allowing the Germans to read six days' worth of Allied traffic.[31] In all, TICOM estimated that the Germans were able to read 10% of the M-209 generated traffic in the European Theater.[32]

The final months of the war put a great strain on the OKH/GdNA as its KONAs retreated back to Germany and its centralized analytic bureaus were forced to evacuate Berlin. Like most German organizations, its operations had largely disintegrated by the time of the surrender.

The largest and newest German signals intelligence service was that of the Air Force. The newly established Luftwaffe relied on the Army for its signal intelligence needs for the first few years, but then established its own service on 1 January 1937, the *Chi* Stelle, OB d L. Starting with one officer and 20 civilians, it grew into an intelligence force of 13,000 by 1945. Its outstanding achievement during the war was what TICOM described as 'signal intelligence without cryptanalysts'. Its skill in interception and traffic

[29]Ibid., p.44.
[30]Ibid., p.49.
[31]TICOM. *Volume 4*, pp.155–7.
[32]R.A. Ratcliff, *Delusions of Intelligence* (New York: Cambridge University Press 2006) p.48.

analysis enabled the *Chi* Stelle to exploit all sorts of Allied radio emissions; radar, navigation beacons and radiotelephone chatter, which created a reputation for yielding valuable tactical and strategic intelligence.[33]

The Air Force sigint service paralleled the army service in that it had a central analysis and administrative center, the *Chi* Stelle, located in Potsdam, and a number of field based Air Signals Regiments and Battalions, attached to the Air Forces on each front. Organizationally the *Chi* Stalle itself divided into a number of geographic evaluation sections along with its administrative departments. Following the German decentralized philosophy, the *Chi* Stalle sent a number of detachments forward to support the field forces, and TICOM concluded 'it was considered more effective to have the long-term evaluation center close to the intercept units rather than close to the staffs which they have to feed'.[34] However, as the war drew on, all of these detachments eventually merged into evaluation companies for the Air Signal regiments and battalions they served.

The cryptanalytic effort on the Russian front was almost entirely field-based, with 85% of the low and medium-grade Russian systems read. The nature of air warfare required a rapid intelligence response, with results needed in a matter of hours rather than days or weeks as with the ground forces. Despite this level of cryptanalytic success with the Russians, the *Chi* Stelle failed to solve other enemy high-grade systems such as SIGABA or Russian one-time pads.

Facing the much more difficult cryptanalytic challenge in the west, the *Chi* Stelle relied heavily on interception and traffic analysis for rapid response. The *Chi* Stalle and its field tactical units became the prime source of intelligence for the Air Raid Warning Agency of the Reich, a function that became critically important as the Anglo-American bombing campaign developed in 1943–45. They developed sophisticated techniques for intercepting Anglo-American radar and navigation systems. Eventually the Germans were able to track the exact strength, composition and probable targets of enemy bomber raids in near real time.[35]

Nevertheless, not all signals intelligence success in the west was due to traffic analysis. *Chi* Stelle assisted in the breaking of the M-209 machine cipher and by spring of 1944, the German Air Force (GAF) was reading six to eight days of encrypted traffic per month. Their reading of M-209 traffic from the US XXIX Tactical Air Command tipped off the Germans to a planned ground offensive in the Aachen area. In addition, many low-level strip systems of both the United States Army Air Force and the Royal Air Force were read, including aircraft movement codes and bomber codes.[36]

Conversely, on the Eastern Front, Air Force sigint could be of great help to the Army. The Russians had a practice of following radio silence prior to a major offensive, their attached air armies however, had to continue to

[33]TICOM, *Volume 5*, pp.1, 9.
[34]Ibid., p.22.
[35]Ibid., p.40.
[36]Ibid., pp.76–9.

coordinate in order to both move their forces and operate their aircraft. This allowed the Luftwaffe signals intelligence service to tip off their ground colleagues to be prepared.[37]

Decentralization however created problems for the *Chi* Stelle. Although it permitted flexibility and an emphasis on tactical intelligence, it diluted any coordinated approach to attacking the high-grade strategic systems of the enemy and the cryptanalysts resented their lack of ability to control intercept targets, which denied them the amount of traffic they needed to work on specific systems. The Luftwaffe signals intelligence effort was under the control of the Chief Signals Officer rather than the intelligence chief, and this created some problems in coordination and emphasis.

Overall, relationships between the three service cryptologic agencies were close. OKW/*Chi* cooperated well with the other armed services, and had some control over the testing and adaption of crypto systems used by the military. However, each branch of the military controlled their own cryptanalysts, and maintained their own independence in signal intelligence matters. Liaison between the Army agency and the OKW/*Chi* was close stemming from their common roots in the old German Defense Ministry, and the fact that both OKW/*Chi* and the OKH/GdNA served under the command of a joint Wehrmacht/Army chief signal officer. In addition, OKW/*Chi* relied on the Army and the other services to provide it with traffic for its own cryptanalytic efforts. Their relationship was one of complete cooperation.[38] Liaison between the Wehrmacht, the Army and the Air Force was for the most part very good, especially in the field between the army and the GAF, where cooperation provided at times great tactical advantages. However, the relationship to the Navy's OKM/4 SKL/III (the B-Dienst)[39] was limited. The GAF's relationship to the Navy was better than the Army's, consisting of tactical cooperation in the field, especially in the Aegean, Black Sea and Baltic areas.[40]

In addition to the four military cryptologic services, there were two civilian agencies, the Foreign Office's Pers ZS[41] and the Nazi Party's Research Bureau, the FA.[42] Both were primarily concerned with diplomatic traffic and at times competed with each other and the OKW/*Chi* in this area. There were turf battles and a lack of cooperation between these agencies at the higher, policy levels; however, at the technical levels there was often cooperation.

The Foreign Office was the oldest, but smallest of the German services, employing between 180 and 200 personnel in 1945. Pers ZS traces its roots back to the Political Intelligence Bureau of the Foreign Office of the immediate post-World War I period. A handful of its 1919 employees were

[37]Ibid., p.92.
[38]Ibid., p.204.
[39]Beobachtungs-Dienst, the Observation Service.
[40]TICOM, *Volume 5*, pp.91–3.
[41]Sonderdienst des Referats Z in der Personaabteilung des Auswaertigen Amtes.
[42]Reichsluftfahrtministeriums/Forschungsamt.

still on the roles of the agency in 1945; thus Pers ZS, although small in number, was highly experienced.[43] Pers ZS was the cryptanalysis branch of the Pers Z section, which also included cryptographic, communications, and administration sections. Their principal effort was the cryptanalysis of foreign diplomatic codes and ciphers, attacking the diplomatic systems of approximately 50 countries and despite its small size it was able to read substantial segments of the medium-grade systems of a number of major powers including England, the United States, France, Italy, China and Japan. According to TICOM, Pers ZS 'evidenced an extraordinary degree of competence'.[44]

The cryptanalytic effort divided between a mathematical subsection and a linguistic-cryptanalytic subsection, further divided into approximately nine groups organized along geographical and linguistic lines. Its greatest success was, ironically on Germany's ally, Italy. Pers ZS was able to read all major Italian diplomatic codes from 1935 until late in 1942. They were also able to read the Japanese 'Red' machine until February 1939, when the traffic became unreadable due to the switch to the 'Purple' machine.

Pers ZS also had one small intercept station, Landhaus in Dahlem, under its control, but OKW/*Chi* and the FA provided the bulk of its intercept traffic. There was no effort given on intercept control or traffic analysis.[45]

Perhaps Per ZS's greatest failure was in the intelligence analysis of its own product. TICOM concluded: 'The organization seemed overly preoccupied with cryptanalysts as a science, and apparently did not think in terms of cryptanalysts as a prime source of intelligence'.[46] The impression given is that Per ZS leaders were professorial types more interested in the problems of decryption than the practical value of the intelligence. There was no central clearinghouse in the organization, and there was divided responsibility with as many as five people involved in the passing of decrypts to the Foreign Office. There was also a lack of feedback and recognition from the Foreign Office, which made it difficult for the cryptanalysts to focus their work.

At the end of 1943, Pers ZS, like the other German intelligence agencies, evacuate Berlin due to the bombings. In the spring of 1945, as the Russians advanced, the Pers ZS groups further splintered and moved to central Germany towards the Burgscheidungen area. Allied intelligence had little information on the Pers ZS organization and was not even certain of its existence until TICOM Team 3 captured it in late April 1945.[47] The TICOM reporters were apologetic about this lack of background information and felt it limited the utility of the intelligence derived from Pers ZS. Many records were destroyed prior to capture and in addition 'the TICOM principle of requiring prisoners to do extensive ''homework'', that is, write

[43]TICOM, *Volume 6*, pp.3 –7.
[44]Ibid., p.25.
[45]TICOM, *Volume 6 – Foreign Office Cryptanalytic Section,* 2–7, pp.19–20.
[46]Ibid., p.56.
[47]Ibid., p.2.

papers, as detailed as possible and in their own words, was not fully developed'.[48]

They did a better job on the other civilian sigint agency, Goering's Research Bureau, the FA. The most unusual fact about the FA was that the existence of this agency was unknown to Allied intelligence until a tipoff given to TICOM during its initial interrogation of Per ZS personnel at Burgscheidungen. On 9 May 1945 TICOM team 1 discovered the abandoned quarters of the FA on the airfield at Kaufbeuren, southwest of Munich, and captured a file of administrative papers revealing the basic details of the organization.[49]

The FA has been described as 'the richest, most secret, the most Nazi, and the most influential of the ... agencies'.[50] Created in 1933 when Gottfried Schapper, a dissatisfied employee of the Defense Ministry cipher bureau, approached Reichsmarschal Herman Goering with the idea of creating a new centralized civilian signals intelligence agency free of the influences of the traditional government ministries. Goering saw this as an opportunity to centralize his own power and approved the creation of a 'Research Bureau' under the cover of the German Air Ministry, but in fact, it was independent of the ministry.[51]

Reporting directly to Goering it functioned as the Nazi Party's sigint agency, its work focused on diplomatic and internal security interception. Before the war the FA was reportedly involved in various Nazi political operations, including the 1934 'blood purge' and the Anschluss (March 1938).[52] As early as 1933, Hitler assigned all telephone monitoring within the Reich to the FA.[53] In addition, they established a deciphering department to work on diplomatic and commercial communications along with a broadcasting monitoring service.

The FA organization consisted of a main office in Berlin and various liaison offices, regional offices and intercept stations. The Berlin office had six main sections dealing with Administration, Personnel, Intercept, Codes and Ciphers, Evaluation, and Technical matters. Each of the main sections contained a number of specialized subsections; for instance, the Technical section had subsections dealing with development of IBM type machinery and another to evaluate captured enemy machinery. The Code and Cipher section did cryptanalysis, and among its successes was the interception and reading of Neville Chamberlain's messages to London during the Munich negotiations, the solving of a Russian teletype machine, and some

[48]Ibid., p.2.
[49]TICOM. *Volume 7*, p.2.
[50]David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (New York: MacMillan Publishing 1978) p.178.
[51]TICOM. *Volume 7*, pp.6–9.
[52]Ibid., p.22.
[53]An example of their product was a book produced in September 1941 that listed the names of all foreign diplomats in Berlin, with whom they were conversing with, and a summary of all their conversations.

commercial systems, including the Swiss Interbank code. The Evaluation section produced the finished intelligence product of the FA, the 'brown reports', which were sent to the highest officials such as Wilhelm Keitel, Karl Doenitz, Joachim von Ribbentrop, and Goering himself.[54] The main office intercept section had two units, one to supervise and administer the FA's intercept efforts, the other a message center to sort and distribute the incoming traffic, employing about 200 people, and operated a large number of small intercept stations throughout Germany. They were of various types, including wireless intercept, teletype and telegraph, telephone intercept, radio broadcasting monitoring, and mail censorship. Much effort pre-war was put into telephone interception; they maintained approximately 1000 telephone taps, half of them in Berlin.[55] However, once the war started and international telephone service became interrupted, the FA had to resort to a greater emphasis on wireless interception.

The FA attacked a number of foreign diplomatic systems, often with the cooperation of the other German sigint agencies. TICOM concluded that the FA possessed copies of a surprising number of foreign codebooks, although there was no information in the documentation as to how the FA acquired them.[56] FA informants stated that some low-grade US systems were read, including a plain five-figure system, the American State Department system, and a Joint American–British system concerned mainly with ship movements. Some British diplomatic systems were read when captured books were available early in the war, and they managed to break the Bank of England code in 1941, in addition to the previously mentioned Interbank code. Most of its work against commercial codes concerned the traffic of German firms to foreign countries prior to the war. Against the Russian target, in addition to a machine teletype code, the FA greatest success was against internal Russian supply and logistic codes. The diplomatic systems of many other minor powers were attacked, including Bulgarian, French, and Italian, Chinese, Finnish, Danish, Japanese and various Latin American systems.

Overall, cryptanalysts supplied less than 20% of the information delivered by the FA, and there was a shift from telephone monitoring to commercial and press traffic as the war progressed.[57]

The relationships between these two civilian agencies and the military services were problematic. The Foreign Office was the senior department in the government and resented OKW/*Chi*'s intrusion into the diplomatic realm; there is no mention of cooperation between the Pers ZS and the Army high command after 1942. Lt. Col. Mettig, head of the Army's sigint service until 1943 and thereafter, second in command at OKW/*Chi*, opposed liaison with the Research Bureau because of his personal opposition to the 'Storm Trooper taint' of the FA.[58] There was antipathy between Goering and von

[54]TICOM, *Volume 7*, p.39.
[55]Kahn, *Hitler's Spies*, p.180.
[56]Ibid., p.74
[57]Ibid., p.72.
[58]TICOM, *Volume 4*, p.210.

Ribbentrop with Goering complaining to his interrogators 'the Foreign Office had continuously tried to interfere' with the FA. These bad relations at the top, however, did not prevent some cooperation among the agencies at the field level.[59]

In addition to the in depth analysis of these five German sigint agencies, TICOM also put an emphasis on the enemy's overall cryptanalytic efforts. They created a detailed listing of all foreign codes attacked by the Germans, providing a description of the code and the degree of success achieved by their code breakers, in an extensive 90-page table. This information reveals that approximately 925 systems of 47 different countries were attacked, with varying degrees of success.[60] Of the primary powers, 122 French systems (including those of Vichy and Free France) were mastered, although many of those were codes and ciphers that were captured after the 1940 defeat. Understandably, Russia was a major target, with 118 systems attacked. Eighty-two British systems were attacked, along with 37 American.[61] Ironically, Germany's allies Italy and Japan were also targets of cryptanalysts. Some of the Pers ZS greatest success was against Italian systems. The effort against Japan, however, failed to break the Japanese high-level Purple machine.[62]

As noted previously, German cryptanalysts were largely successful against low- and medium-grade systems, which often produced information of great tactical use, especially on the Eastern Front. Against the west, the most important systems broken by the Germans were some of the British naval codes, including the Naval Cipher No. 3, the British and Allied Merchant Ships (BAMS) code. They had some success with breaking and reconstructing scrambled telephony, especially that intercepted by the Forschungsstelle, the 'Research Post' of the German Postal Ministry. Their intercept station at Valkenswaard, in the Netherlands, monitored AT&T's New York–London circuit, recording anywhere from 30 to 60 phone conservations a day, including those between Roosevelt and Churchill.[63] However, cautious use of the phone by allied users limited the usefulness to the Germans of the intelligence derived from this source.[64]

TICOM also looked at the German's cryptologic efforts to secure their own systems. Their failure to secure the Enigma machine is now legendary; although they knew from theoretical studies that the machine had weakness, they never put in the practical effort to convince themselves of the need to change the system. The Germans knew that some of the earlier models of the Enigma were insecure, but the latter models utilizing a plug board, and the

[59]TICOM, *Volume 3,* pp.90–102.
[60]TICOM, *Volume 1*, Chart summarizing results of European Axis Cryptanalysts.
[61]Ibid.
[62]Bruce Lee, *Marching Orders: The Untold Story of World War II* (New York: Crown Publishers 1995).
[63]Kahn, *Hitler's Spies*, pp.173–6.
[64]Patrick D. Weadon, *Sigsaly Story*, National Security Agency/Central Security Service, 2009, <http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/sigsaly_story.shtml> (accessed 30 August 2010).

Navy model with a fourth rotor became standard and were thought to be secure if used properly (they were not). By the end of the war, improved models of the Enigma were under development using variable-notch rotors, rather than the more predictable one- or two-notch rotors previously used. This would have increased the mathematical possibilities of the machine beyond the capabilities of the Allied cryptanalysts. If this version of the machine had been introduced as planned in 1943, it would have blacked out Ultra. However, lack of clarity in operational requirements, and pure technical difficulties delayed the introduction of new models of the Enigma machine.

The story was similar in the German use of secure teletypewriter circuits. This technology was developed in the 1920s and 1930s for commercial and press requirements for long distance communications. Utilizing machine generated five-bit machine Bardot code, it enabled the rapid and accurate transmission of text. Unlike the Enigma machine, which required two code clerks to encrypt a message and a radioman to transmit it via Morse code, the plaintext message, typed onto paper tape and then run through a reader, automatically generated and transmitted the encrypted text. All the major powers adopted this technology for encrypted diplomatic and military traffic. Teletype circuits were often landline-based between major headquarters; however, as the war progressed and the fronts first expanded and then retreated, the Germans were forced to put these circuits on the radio. This gave the British the opportunity to intercept them, and then after a massive effort, break them. This intelligence was code named FISH. The Germans had two types of teletypewriter systems; the first consisted of a teleprinter cipher attachments, the SZ-42 (codenamed 'Tunny' by the British), and the T-52 *Geheimschreiber* series of machines in which the cryptographic mechanisms were integral to the teleprinter (British codename 'Sturgeon'). Bletchley Park developed the Colossus, considered the world's first programmable digital computer, to break this system. Developments late in the war, including the SZ-42c which streamed the data continuously, thus making it impervious to traffic analysis, and advance versions of the *Geheimschreiber* machines, the T-52d and the T-52e, would have blacked out Fish.[65] Like the advanced Enigma machines, these developments came too late in the war for widespread use.

Nevertheless, how successful was TICOM in meeting its four targeted goals? Its first and major goal, to learn the extent of the German cryptanalytic effort against England and America, was highly reassuring. TICOM confirmed that at no time did the Germans successfully attack any of the highest-level British–American systems, those encoded with either the TYPEX or the SIGABA machines. The Germans never tapped into the sort of enemy strategic communications that the Allied enjoyed from Ultra.[66]

Serious efforts were attempted theater-wide to achieve the second goal, to prevent the results of such German cryptanalysis from falling into

[65]TICOM, *Volume 2*, Chapter 3.
[66]TICOM, *Volume 1*, p.5.

unauthorized hands. There was a standing order from SHAEF (Supreme Headquarters Allied Expeditionary Force) to both Sixth and Twelfth Army groups to provide special handling to any captured German signal intelligence units. Custody of a captured unit or site was to be turned over to the nearest Allied sigint unit, which was then ordered to seal it and establish a guard until an appropriate TICOM unit could inspect it.[67] However, given the chaos of the closing days of the war, it is impossible to know how much material was burned by the Germans, looted by Allied troops, or captured by the Russians.

The third goal, to exploit German cryptologic techniques and inventions was a great success; a substantial volume of material was captured intact. TICOM reported the seizure of 4000 separate German cryptologic documents consisting of correspondence, messages, films, worksheets or other items of intelligence value; in all a treasure trove weighing five tons. In addition, TICOM and other allied intelligence units conducted scores of interviews with former German sigint personnel. The preliminary analysis of this material yielded at least 196 TICOM reports that were the basis for the writing of the 1946 ASA study.[68] The exploitation of the German information on Soviet low- and medium-level codes and the information provided about traffic analysis techniques against the Russians alone would have been of invaluable assistance in the early days of the Cold War. It is fair to conclude that between May 1945 and May 1946 the Allies learned as much as possible about Axis signals intelligence given the resources at the time.

The final goal to uncover items of signal intelligence value in the prosecuting the war against Japan turned out to be not as important as originally assumed. There was great fear among Allied intelligence that the Germans were closely cooperating with the Japanese and transferring crypto data and machinery to Japan, much as they were in providing jet and rocket technology. However, TICOM reveals that the cryptologic relationship between Germany and Japan was almost non-existent, except for a rare occasional visit from Japanese military attachés to OKW/*Chi*. The only serious effort at cooperation happened late in the war when plans were made to send a small delegation of German Army and Navy cryptanalysts to Japan by submarine. Nevertheless, as stated in the TICOM study 'so little was known about Japanese cryptanalytic activity that the delegation did not know where they were to go in Japan or to whom they should announce their arrival'.[69] The conquest of Germany and the rapid ending of the Japanese war made the whole threat moot.

By the time TICOM completed its analysis in the spring of 1946, the Russian problem became a major concern for the Anglo-American intelligence services. Although not one of the original goals, by this time TICOM had put additional emphasis on the Germans' experience with Soviet communications, adding additional chapters on Russian ciphers and

[67]Ibid., p.4.
[68]TICOM, *Volume 8*, p.61.
[69]TICOM, *Volume 3*, p.105.

an additional volume on traffic analysis, indicating a growing concern by the ASA on what would soon be labeled 'the cold war'. However, when it came to success against Soviet diplomatic and high-level ciphers, which relied on the use of one-time pads, the Germans had no greater success than the Allies did. Both the Foreign Office's Per ZS and OKW/*Chi* apparently gave up early on Russian diplomatic traffic.[70] More was accomplished against high-level Russian Baudot traffic. In 1943, the FA had some success studying a five-impulse Bardot system and had recreated the action of the teletype machine, but this effort ended when the Russians altered the system. In a rare example of cooperation, the FA communicated the results of its investigations to the mathematical section of the Army's GdNA, and by 1945, its Group VI was regularly reading high-level Baudot traffic between the Russian general staff to its Army Front staff and its Assault Armies.[71] The Germans built a custom-built receiver, 'the Russian Fish', to intercept this traffic, which after capture by TICOM, was sent back to England with its crew to be set up at Wavendon Manor, an outstation of Bletchley Park. This produced a stream of intelligence code-named 'Caviar' by the British.[72] Bamford states that the capture and the exploitation of the Russian Fish machine was a major reason that TICOM remained classified all these years.[73]

Perhaps the greatest mystery of TICOM is why it remained a secret for so long. The captured materials sent to Britain were processed and microfilmed, with copies provided to the Americans. Translations, intelligence reports and the nine-volume executive TICOM study were completed by the spring of 1946. This TICOM study revealed the vulnerability of many smaller countries' codes and ciphers to cryptanalytic attack, and since after the war Britain and the United States continued to be interested in reading all these systems, this information needed to be kept classified. However, the Soviet Union changed all their codes and ciphers in 1948 because of William Weisband's betrayal, an event known as 'Black Friday' to the NSA, which resulted in a 30-year blackout of Russian systems.[74] By the mid-1970s, Enigma-type crypto machines had become technologically obsolete, with most countries switching to more modern solid state, and later computer/software-based systems. By the mid-1990s, individuals, with the use of microcomputers and readily available software, could utilize cryptologic systems that far exceeded the capabilities of the World War II era. Because of these changes, the British government in 1974 allowed F.W. Winterbotham to publish *The Ultra Secret*, bringing to public awareness the existence and

[70]TICOM, *Volume 6*, p.31.
[71]TICOM, *Volume 4*, pp.65, 211.
[72]Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Harper Press 2010) p.49.
[73]Bamford, *Body of Secrets*, p.17.
[74]Matthew M. Aid, *The Secret Sentry: The Untold History of the National Security Agency* (New York: Bloomsbury Press 2009) pp.7–19.

scope of World War II's signal intelligence effort.[75] With the flood of historical accounts and studies that followed, and with the US government's own declassification of Ultra, Magic, and the post-war VENONA program, the need to maintain any general secrecy around signals intelligence seems unnecessary.

Nevertheless, in 1992 the Director of the NSA extended its classification until the year 2012.[76] However, the various volumes were declassified and released prior to 2012, beginning in 1998, and the rest in 2008 and 2009, reportedly at the request of historian David Alvarez.[77]

The nine volumes of the 1946 ASA TICOM study are now available to the public. However, the supporting intelligence reports are scattered among the NSA archives and the National Archives and Records Administration (NARA), creating another problem of access for researchers. NSA does not provide a public catalog; requests need to be made through the Freedom of Information Act (FOIA) office to confirm the existence of these documents. A number of TICOM-related reports, although declassified and turned over to NARA, are not listed in the NARA public catalog. Hopefully, this just reflects a lag in NARA's cataloging backlog. Other TICOM materials are available in the British National Archives and in Germany's Foreign Office Archives.[78] The ability of researchers to reconstruct the entire TICOM archive is of some historic value, as it will pinpoint what US intelligence knew pertaining to cryptology in the early days of the cold war. Ironically, until NSA completes its TICOM releases, and NARA catalogs these items, they are likely to remain as obscure as they were when classified, and the secrets of TICOM will continue to puzzle historians.

Postscript

The April 2011 NSA release of over 50,000 declassified pages to NARA College Park facility contained over 600 TICOM-related documents. See RG 457, Entry P 3 'Historians' Source Files Relating to Wilhelm Flicke', Entry P 4 'Historians' Source Files Relating to Target Intelligence Committee (TICOM) Interrogation Reports', and Entry P 11 'Archival and Historian's Source Files'. Some of these documents can be found online at the author's website, The TICOM Archive (https://sites.google.com/site/ticomarchive/).

[75]Winterbotham, *The Ultra Secret*.
[76]Bamford, *Body of Secrets*, p.8.
[77]Shlomo Aronson, *Hitler, the Allies and the Jews* (Cambridge: Cambridge University Press 2004) 336.
[78]David Kahn, 'The *Fonds de Moscou*, TICOM, and the Nerve of a Spy', *Intelligence and National Security* 24/6 (2009) pp.865–75.